ПСВ

Числа $a_1, \ldots, a_n$ образуют полную систему вычетов по модулю m (сокращенно: ПСВ $\pmod m$), если каждый вычет по модулю м содержит ровно одно из них.

ПСВ

Числа $a_1, \ldots, a_n$ образуют полную систему вычетов по модулю m (сокращенно: ПСВ $\pmod{m}$), если каждый вычет по модулю м содержит ровно одно из них.

Пример:

Пусть $m = 7$, тогда ПСВ может иметь вид:

$0, 1, 2, 3, 4, 5, 6$

$\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$

Теоремы для ПСВ

Теорема: пусть $a_1, \ldots, a_m$ – ПСВ $\pmod{m}, k, b \in \mathbb{Z}$, причем $(k, m) = 1$. Тогда домножить все a_i и добавить к ним b и получить ПСВ.

Теоремы для ПСВ

Теорема: пусть $a_1, \ldots, a_m$ – ПСВ $\pmod m$, $k, b \in \mathbb{Z}$, причем $(k, m) = 1$.
Тогда домножить все a_i и добавить к ним b и получить ПСВ.

Доказательство:

Нужно проверить, что никакие два элемента не сравнимы по модулю m.

Пусть $ka_i + b \equiv_m ka_j + b \Leftrightarrow k(a_i - a_j) \,\vdots\, m$.

Теоремы для ПСВ

Теорема: пусть $a_1, \ldots, a_m$ – ПСВ $\pmod m), k, b \in \mathbb{Z}$, причем $(k, m) = 1$.
Тогда домножить все a_i и добавить к ним b и получить ПСВ.

Доказательство:

Нужно проверить, что никакие два элемента не сравнимы по модулю m.

Пусть $ka_i + b \equiv_m ka_j + b \Leftrightarrow k(a_i - a_j) \,\vdots\, m$.

Но так как $(k, m) = 1$, то $a_i - a_j \,\vdots\, m \Leftrightarrow a_i \equiv_m a_j$, что явно не так.

ПрСВ $\pmod m$

Числе $a_1, \ldots, a_{\phi(m)}$ образуют приведенную систему вычетов по модулю m, (сокращенно: ПрСВ $\pmod m$), если каждый вычет взаимно прост с m.

ПрСВ $\pmod m$

Числе $a_1, \ldots, a_{\phi(m)}$ образуют приведенную систему вычетов по модулю m, (сокращенно: ПрСВ $\pmod m$), если каждый вычет взаимно прост с m.

Теорема: пусть $a_1, \ldots, a_{\phi(m)}$ – ПрСВ $\pmod m$, $k \in \mathbb{Z}$, причем $(k, m) = 1$.

Тогда $ka_1, \ldots, ka_{\phi(m)}$ – ПрСВ $\pmod m$.

ПрСВ $\pmod m$

Числе $a_1, \ldots, a_{\phi(m)}$ образуют приведенную систему вычетов по модулю m, (сокращенно: ПрСВ $\pmod m$), если каждый вычет взаимно прост с m.

Теорема: пусть $a_1, \ldots, a_{\phi(m)}$ – ПрСВ $\pmod m), k \in \mathbb{Z}$, причем $(k, m) = 1$.

Тогда $ka_1, \ldots, ka_{\phi(m)}$ – ПрСВ $\pmod m$.

Доказательство:

Нужно проверить, что все получившиеся вычеты взаимно просты и никакие два из них несравнимы.

ПрСВ $\pmod m$

Числе $a_1, \ldots, a_{\phi(m)}$ образуют приведенную систему вычетов по модулю m, (сокращенно: ПрСВ $\pmod m$), если каждый вычет взаимно прост с m.

Теорема: пусть $a_1, \ldots, a_{\phi(m)}$ – ПрСВ $\pmod m), k \in \mathbb{Z}$, причем $(k, m) = 1$.

Тогда $ka_1, \ldots, ka_{\phi(m)}$ – ПрСВ $\pmod m$.

Доказательство:

Нужно проверить, что все получившиеся вычеты взаимно просты и никакие два из них несравнимы.

То, что они не сравнимы было доказана ранее, докажем взаимную простоту.

ПрСВ $\pmod m$

Числе $a_1, \ldots, a_{\phi(m)}$ образуют приведенную систему вычетов по модулю m, (сокращенно: ПрСВ $\pmod m$), если каждый вычет взаимно прост с m.

Теорема: пусть $a_1, \ldots, a_{\phi(m)}$ – ПрСВ $\pmod m$, $k \in \mathbb{Z}$, причем $(k, m) = 1$.

Тогда $ka_1, \ldots, ka_{\phi(m)}$ – ПрСВ $\pmod m$.

Доказательство:

Нужно проверить, что все получившиеся вычеты взаимно просты и никакие два из них несравнимы.

То, что они не сравнимы было доказана ранее, докажем взаимную простоту.

Если $(k, m) = 1$ и $(a_i, m) = 1$, то $(ka_i, m) = 1$ для всех $i \in \{1, \ldots, \phi(m)\}$.

Примеры ПРсВ

Пусть $m = 7$

Примеры ПРсВ

Пусть $m = 7$

$0, 1, 2, 3, 4, 5, 6$

Примеры ПРсВ

Пусть $m = 7$

$0, 1, 2, 3, 4, 5, 6$

Пусть $m = 6$

Примеры ПРсВ

Пусть $m = 7$

$0, 1, 2, 3, 4, 5, 6$

Пусть $m = 6$

$1, 4, 5$

Примеры ПРсВ

Пусть $m = 7$

$0, 1, 2, 3, 4, 5, 6$

Пусть $m = 6$

$1, 4, 5$

0 – НЕ ВХОДИТ

1 – ВХОДИТ